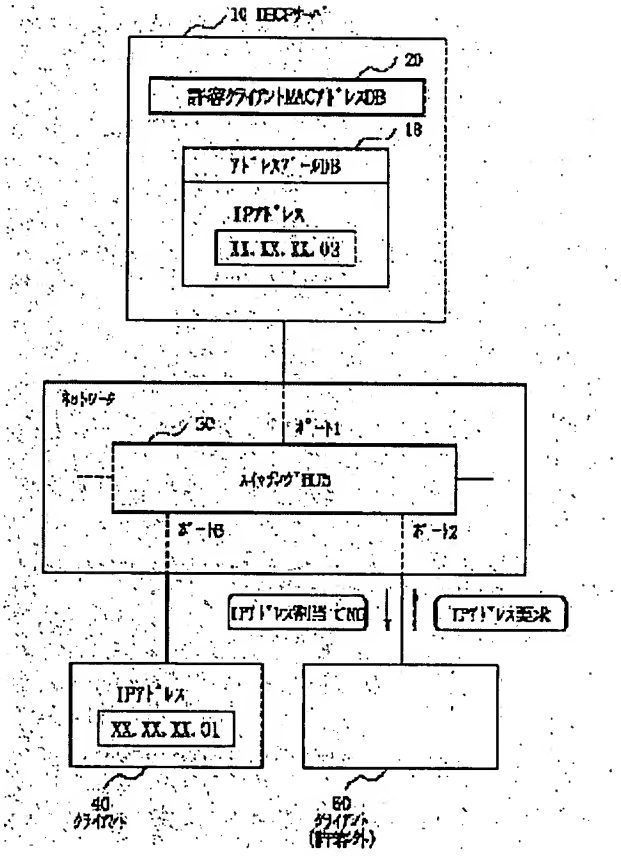
DHCP SERVER WITH CLIENT AUTHENTICATING FUNCTION AND AUTHENTICATING METHOD THEREOF

Publication number: JP2001211180
Publication date: 2001-08-03
Inventor: MORIYA MASAMI
Applicant: NEC COMMUNICATION SYST
Classification:
- international: ***H04L9/32; H04L12/28; H04L12/56;*** **H04L9/32; H04L12/28; H04L12/56;** (IPC1-7): H04L12/28; H04L9/32; H04L12/56
- European:
Application number: JP20000017668 20000126
Priority number(s): JP20000017668 20000126

Abstract of **JP2001211180**

PROBLEM TO BE SOLVED: To provide high security by equipping a DCHP server with a function of authenticating an IP-address assigned client and releasing an IP address when an unallowed client is found and a function of reporting communication rejection. SOLUTION: The DHCP server 10 when receiving requests to assign IP addresses from clients 40 and 60 checks whether or not their MAC addresses are registered in an allowed client MAC address DB 20, and allocates and records the IP addresses in an allocated-address DB while making them correspond to the MAC addresses when they are registered. Then an ARP packet is sent periodically to the IP addresses and it is checked whether or not a combination of the transmission source MAC address and the transmission source IP address in its response packet is recorded in the allocated address database, when it is recorded, a regular client is decided and when not, an irregular client is decided.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－211180
（Ｐ２００１－２１１１８０Ａ）
(43)公開日　平成13年８月３日(2001.8.3)

(51)Int.Cl.[7]	識別記号	ＦＩ			テーマコード（参考）
H04L 12/28		H04L 11/00	310	Z	5J104
9/32		9/00	673	B	5K030
12/56		11/20	102	Z	5K033

審査請求　有　請求項の数７　ＯＬ　（全８頁）

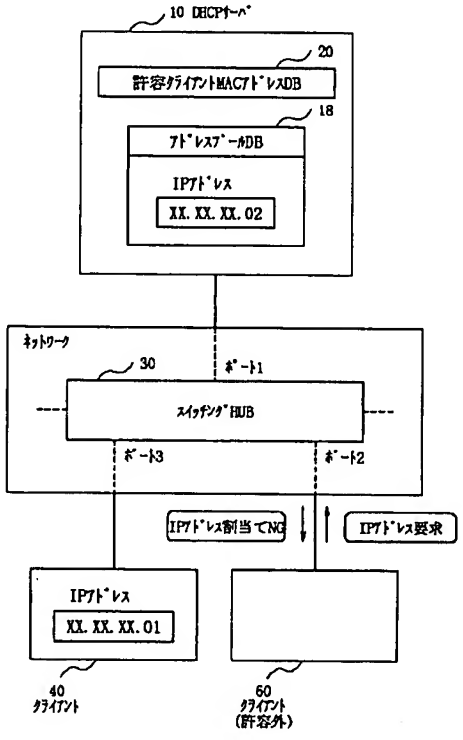
(21)出願番号　特願2000－17668（Ｐ2000－17668）
(22)出願日　平成12年１月26日(2000.1.26)

(71)出願人　000232254
日本電気通信システム株式会社
東京都港区三田１丁目４番28号
(72)発明者　森谷　真佐美
東京都港区三田一丁目４番28号　日本電気通信システム株式会社内
(74)代理人　100082935
弁理士　京本　直樹　（外２名）

Ｆターム(参考)　5J104 AA07 KA02 NA21 PA07
5K030 GA15 HC14 KA02
5K033 AA08 CB08 EC04
9A001 BB02 BB03 BB04 CC06 CC07
DD10 JJ01 JJ18 JJ25 JJ27
KK56 LL03 LL09

(54)【発明の名称】クライアント認証機能付きＤＨＣＰサーバ、及びその認証方法

(57)【要約】
【課題】ＤＨＣＰサーバにおいて、ＩＰアドレスの取得希望／取得済みクライアントの正規性を確認する。
【解決手段】ＤＨＣＰサーバ１０は、クライアント４０，６０からのＩＰアドレスの割当て要求を受けると、そのＭＡＣアドレスが許容クライアントＭＡＣアドレスＤＢ２０に登録されているか照合し、登録されていればＩＰアドレスを割当てＭＡＣアドレスと対応付けて割当て済みアドレスＤＢに記録する。その後、定期的に当該ＩＰアドレスへＡＲＰパケットを送信し，その応答パケット中の送信元ＭＡＣアドレス及び送信元ＩＰアドレスの組合わせが割当て済みアドレスデータベースに記録されているか照合し、記録されていれば正規クライント、記録されていなければ不正規クライントと判定する。



1

【特許請求の範囲】

【請求項１】　ネットワーク接続されたクライアントからの要求を受けＩＰアドレスの動的割当てを行うＤＨＣＰサーバにおいて、

ＩＰアドレスの割当て許容対象のクライアントのＭＡＣアドレスをあらかじめ登録した許容クライアントＭＡＣアドレスデータベースと、割当て済みのＩＰアドレスとＭＡＣアドレスとを対応付けて記録するための割当て済みアドレスデータベースとを有し、

クライアントからのＩＰアドレスの割当てを要求するメッセージを受けると、当該メッセージ中の送信元ＭＡＣアドレスが前記許容クライアントＭＡＣアドレスデータベースに登録されているか照合し、登録されているときのみ使用可能なＩＰアドレスを割当てて当該クライアントに通知するとともに、当該ＭＡＣアドレスと対応付けて前記割当て済みアドレスデータベースに記録し、前記ＩＰアドレスの割当て後、定期的に当該ＩＰアドレスのクライアントに対して当該クライアントのＭＡＣアドレスを含む応答メッセージの返信を要求するメッセージを送信し、当該応答メッセージ中の送信元ＭＡＣアドレス及び送信元ＩＰアドレスの組合わせが前記割当て済みアドレスデータベースに記録されているか照合し、照合結果に基づいて当該クライアントが正規にＩＰアドレスを割当てられたクライントであるか否かを判定することを特徴とするクライアント認証機能付きＤＨＣＰサーバ。

【請求項２】　前記クライアントからの応答メッセージ中の送信元ＭＡＣアドレス及び送信元ＩＰアドレスの組合わせの前記割当て済みアドレスデータベースによる照合の結果、当該組合せが記録されていなければ、当該クライアントが正規にＩＰアドレスを割当てられたクライントではないと判定し、当該ＩＰアドレスの割当てを取消すとともに、当該クライアントに対し強制ＩＰアドレス解放通知メッセージを送信することを特徴とする請求項１記載のクライアント認証機能付きＤＨＣＰサーバ。

【請求項３】　前記クライアントからの応答メッセージ中の送信元ＭＡＣアドレス及び送信元ＩＰアドレスの組合わせの前記割当て済みアドレスデータベースによる照合結果に基づいて、当該クライアントが正規にＩＰアドレスを割当てられたクライントではないと判定した場合に、当該クライアントをネットワークに接続するためのスイッチングハブ装置に対し、当該ＭＡＣアドレスに対する通信を行わないよう設定させることを特徴とする請求項１記載のクライアント認証機能付きＤＨＣＰサーバ。

【請求項４】　請求項３記載のクライアント認証機能付きＤＨＣＰサーバとクライアントとを収容し、前記クライアント認証機能付きＤＨＣＰサーバからの制御情報を登録する手段と、登録された制御情報に応じて前記クライアントの他のネットワーク構成要素との間の通信の可否を制御するスイッチ手段とを有することを特徴とするスイッチングハブ装置。

2

【請求項５】　ネットワーク接続されたクライアントからの要求を受けＩＰアドレスの動的割当てを行うＤＨＣＰサーバのクライアント認証方法において、

クライアントからのＩＰアドレスの割当てを要求するメッセージを受けると、当該メッセージ中の送信元ＭＡＣアドレスがＩＰアドレスの割当て許容対象のクライアントのＭＡＣアドレスをあらかじめ登録した許容クライアントＭＡＣアドレスデータベースに登録されているか照合し、登録されているときのみ使用可能なＩＰアドレスを割当てて当該クライアントに通知するとともに、当該ＭＡＣアドレスと対応付けて割当て済みアドレスデータベースに記録し、前記ＩＰアドレスの割当て後、定期的に当該ＩＰアドレスのクライアントに対して当該クライアントのＭＡＣアドレスを含む応答メッセージの返信を要求するメッセージを送信し、当該応答メッセージ中の送信元ＭＡＣアドレス及び送信元ＩＰアドレスの組合わせが前記割当て済みアドレスデータベースに記録されているか照合し、照合結果に基づいて当該クライアントが正規にＩＰアドレスを割当てられたクライントであるか否かを判定することを特徴とするクライアント認証方法。

【請求項６】　前記クライアントからの応答メッセージ中の送信元ＭＡＣアドレス及び送信元ＩＰアドレスの組合わせの前記割当て済みアドレスデータベースによる照合の結果、当該組合せが記録されていなければ、当該クライアントが正規にＩＰアドレスを割当てられたクライントではないと判定し、当該ＩＰアドレスの割当てを取消すとともに、当該クライアントに対し強制ＩＰアドレス解放通知メッセージを送信することを特徴とする請求項５記載のクライアント認証方法。

【請求項７】　前記クライアントからの応答メッセージ中の送信元ＭＡＣアドレス及び送信元ＩＰアドレスの組合わせの前記割当て済みアドレスデータベースによる照合結果に基づいて、当該クライアントが正規にＩＰアドレスを割当てられたクライントではないと判定した場合に、当該クライアントをネットワークに接続するためのスイッチングハブ装置に対し、当該ＭＡＣアドレスに対する通信を行わないよう設定させることを特徴とする請求項５記載のクライアント認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はクライアント認証機能付きＤＨＣＰサーバ、及びその認証方法に関し、特にネットワーク接続されたクライアントからの要求を受けＩＰアドレスの動的割当てを行うＤＨＣＰサーバと、その制御の下、クライアントの他のネットワーク構成要素との間の通信の可否を制御するスイッチングハブ装置と、そのクライアント認証方法とに関する。

【０００２】

【従来の技術】ＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）はネットワーク内のシステムのＩＰアドレスを一元管理することができるＵＤＰ上のプロトコルで、クライアント／サーバ方式を採用している。通常、ＤＨＣＰサーバは同一サブネット毎に設置され、クライアントの要求に応じてＩＰアドレスの動的割当てを行っている。それにより、クライアントは個別にＩＰアドレスの設定を行うことなく、ＴＣＰ／ＩＰ通信を行うことができる。

【０００３】

【発明が解決しようとする課題】しかし、上述した従来のＤＨＣＰサーバは、動的割当ての利点がある反面、ＩＰアドレスを割当てる際にクライアントに対しての認証は一切行っていない。そのため、ネットワークに接続してしまえば、どのようなクライアントでもＩＰアドレスを取得し、通信を行ってしまうことができてしまう。これはセキュリティ上重大な問題である。また、ＩＰアドレスを新規に取得する以外にも、他の正規クライアントのＩＰアドレスを盗む場合があり、この場合でもクライアントの正規性を確認することができない。

【０００４】本発明は、これらの問題を解決するために、ＤＨＣＰサーバにＩＰアドレス割当てクライアントの認証及び許容外クライアント発見時のＩＰアドレス解放通知機能、通信拒否通知機能を具備させることで高いセキュリティを提供する。

【０００５】

【課題を解決するための手段】本発明のクライアント認証機能付きＤＨＣＰサーバは、ネットワーク接続されたクライアントからの要求を受けＩＰアドレスの動的割当てを行うＤＨＣＰサーバにおいて、ＩＰアドレスの割当て許容対象のクライアントのＭＡＣアドレスをあらかじめ登録した許容クライアントＭＡＣアドレスデータベースと、ＩＰアドレスとＭＡＣアドレスとを対応付けて記録するための割当て済みアドレスデータベースとを有し、クライアントからのＩＰアドレスの割当てを要求するメッセージを受けると、当該メッセージ中の送信元ＭＡＣアドレスが前記許容クライアントＭＡＣアドレスデータベースに登録されているか照合し、登録されているときのみ使用可能なＩＰアドレスを割当てて当該クライアントに通知するとともに、当該ＭＡＣアドレスと対応付けて前記割当て済みアドレスデータベースに記録し、前記ＩＰアドレスの割当て後、定期的に当該ＩＰアドレスのクライアントに対して当該クライアントのＭＡＣアドレスを含む応答メッセージの返信を要求するメッセージを送信し、当該応答メッセージ中の送信元ＭＡＣアドレス及び送信元ＩＰアドレスの組合わせが前記割当て済みアドレスデータベースに記録されているか照合し、照合結果に基づいて当該クライアントが正規にＩＰアドレスを割当てられたクライントであるか否かを判定する構成である。

【０００６】また、上記構成において、前記クライアントからの応答メッセージ中の送信元ＭＡＣアドレス及び送信元ＩＰアドレスの組合わせの前記割当て済みアドレスデータベースによる照合の結果、当該組合せが記録されていなければ、当該クライアントが正規にＩＰアドレスを割当てられたクライントではないと判定し、当該ＩＰアドレスの割当てを取消すとともに、当該クライアントに対し強制ＩＰアドレス解放通知メッセージを送信する構成とすることができる。

【０００７】あるいは、前記クライアントからの応答メッセージ中の送信元ＭＡＣアドレス及び送信元ＩＰアドレスの組合わせの前記割当て済みアドレスデータベースによる照合結果に基づいて、当該クライアントが正規にＩＰアドレスを割当てられたクライントではないと判定した場合に、当該クライアントをネットワークに接続するためのスイッチングハブ装置に対し、当該ＭＡＣアドレスに対する通信を行わないよう設定させる構成とすることができる。

【０００８】本発明のスイッチングハブ装置は、上記構成のクライアント認証機能付きＤＨＣＰサーバとクライアントとを収容し、前記クライアント認証機能付きＤＨＣＰサーバからの制御情報を登録する手段と、登録された制御情報に応じて前記クライアントの他のネットワーク構成要素との間の通信の可否を制御するスイッチ手段とを有する。

【０００９】本発明のクライアント認証方法は、ネットワーク接続されたクライアントからの要求を受けＩＰアドレスの動的割当てを行うＤＨＣＰサーバのクライアント認証方法において、クライアントからのＩＰアドレスの割当てを要求するメッセージを受けると、当該メッセージ中の送信元ＭＡＣアドレスがＩＰアドレスの割当て許容対象のクライアントのＭＡＣアドレスをあらかじめ登録した許容クライアントＭＡＣアドレスデータベースに登録されているか照合し、登録されているときのみ使用可能なＩＰアドレスを割当てて当該クライアントに通知するとともに、当該ＭＡＣアドレスと対応付けて割当て済みアドレスデータベースに記録し、前記ＩＰアドレスの割当て後、定期的に当該ＩＰアドレスのクライアントに対して当該クライアントのＭＡＣアドレスを含む応答メッセージの返信を要求するメッセージを送信し、当該応答メッセージ中の送信元ＭＡＣアドレス及び送信元ＩＰアドレスの組合わせが前記割当て済みアドレスデータベースに記録されているか照合し、照合結果に基づいて当該クライアントが正規にＩＰアドレスを割当てられたクライントであるか否かを判定する工程を有する。

【００１０】また、上記工程において、前記クライアントからの応答メッセージ中の送信元ＭＡＣアドレス及び送信元ＩＰアドレスの組合わせの前記割当て済みアドレスデータベースによる照合の結果、当該組合せが記録されていなければ、当該クライアントが正規にＩＰアドレ

スを割当てられたクライントではないと判定し、当該ＩＰアドレスの割当てを取消すとともに、当該クライアントに対し強制ＩＰアドレス解放通知メッセージを送信する工程を含むことができる。

【００１１】あるいは、前記クライアントからの応答メッセージ中の送信元ＭＡＣアドレス及び送信元ＩＰアドレスの組合わせの前記割当て済みアドレスデータベースによる照合結果に基づいて、当該クライアントが正規にＩＰアドレスを割当てられたクライントではないと判定した場合に、当該クライアントをネットワークに接続するためのスイッチングハブ装置に対し、当該ＭＡＣアドレスに対する通信を行わないよう設定させる工程を含むことができる。

【００１２】

【発明の実施の形態】まず、本発明の概要を説明する。本発明のクライアント認証機能付きＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）サーバは、ＩＰアドレスの動的割当てを行う場合に発生しうる、なりすましを防止するためのクライアント認証機能を具備し、セキュリティを向上させることを特徴としている。「なりすまし」とは、不正なクライントが、あたかもネットワーク内の正規のクライアントであるかのようにして、ＩＰアドレスを取得することをいう。

【００１３】次に、本発明の実施の形態について図面を参照して詳細に説明する。

【００１４】図１は本発明の一実施の形態を示すＤＨＣＰサーバを用いたネットワークの構成図である。図１を参照すると、サブネット内にＤＨＣＰサーバ１０が設定され、スイッチングＨＵＢ（ハブ装置）３０を含む伝送路を介して接続された複数のクライアント（４０及び６０のみ図示）に対し、ＩＰアドレスの動的割当てを行っているネットワークである。

【００１５】ＤＨＣＰサーバ１０の許容クライアントＭＡＣアドレスＤＢ（データベース）２０にはＩＰアドレス割当てを許容するクライアントのＭＡＣアドレスが、アドレスプールＤＢ（データベース）１８には割当て可能なＩＰアドレス（ＸＸ．ＸＸ．ＸＸ．０２）が記録されている。

【００１６】現在、クライアント４０は許容クライアントで、そのＭＡＣアドレスがＤＨＣＰサーバ１０の許容クライアントＭＡＣアドレスＤＢ２０に記録され、ＩＰアドレス（ＸＸ．ＸＸ．ＸＸ．０１）が割当てられているものとする。クライアント６０は許容外のクライアントで、ＭＡＣアドレスはＤＨＣＰサーバ１０の許容クライアントＭＡＣアドレスＤＢ２０に記録されていない。

【００１７】この状態でＤＨＣＰサーバ１０が、クライアント６０からサーバ検索要求を受信した場合、許容クライアントＭＡＣアドレスＤＢ２０とクライアント６０のＭＡＣアドレスとの比較を行う。この比較で一致しなければ、ＤＨＣＰサーバ１０はＩＰアドレスの割当て不能を示すＮＧ情報をクライアント６０に送信し、ＩＰアドレスの割当ては行わない。しかし、これで全てのなりすまし防止を行うことはできていない。

【００１８】ここで、正規ＩＰアドレスを取得した許容クライアント４０の場合を例に、ＩＰアドレスの取得手順を説明する。許容クライアントの認証後、ＤＨＣＰサーバ１０は、ＩＣＭＰ（Ｉｎｔｅｒｎｅｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅ Ｐｒｏｔｏｃｏｌ）のＥｃｈｏメッセージをアドレスプールＤＢ１８から選択したＩＰアドレス（ＸＸ．ＸＸ．ＸＸ．０１（この時点ではまだ未使用））に対して送付する。未使用であることを確認後、アドレスをクライアント４０に提示し、クライアント４０はそのアドレスを要求する。その後、ＤＨＣＰサーバ１０は正式にＩＰアドレスの割当てを行う。

【００１９】確かにクライアント４０は許容クライアントでＩＰアドレスの割当ても正常に行われている。しかし、ここで問題が生じる。許容クライアント４０がＩＰアドレスを取得したあとに、そのアドレスを他のクライアントが盗む可能性があるということである。

【００２０】それを回避する方法として、定期的に割当て済みの全てのアドレスに対してＡＲＰ（Ａｄｒｅｓｓ Ｒｅｓｏｌｕｔｉｏｎ Ｐｒｏｔｏｃｏｌ）パケットを送付する。その応答によって得られるＭＡＣ（Ｍｅｄｉａ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ）アドレスによりなりすましクライアントを発見することができる。

【００２１】そして、実際になりすましクライアントを発見した場合には、ＤＨＣＰサーバ１０は、割当てを認識していないクライアント（例えばクライアント６０）に対して強制ＩＰアドレス解放通知を送付する。

【００２２】しかし、この強制ＩＰアドレス解放通知は通知のみで、ＩＰアドレスの解放はクライアント側に依存してしまう。そのため、実際に解放されることはまず無いと考えた方がよい。

【００２３】よって、入出力ポート間でＭＡＣアドレスによるパケットデータのスイッチングを行うスイッチング手段（図示せず）を有するスイッチングＨＵＢ３０に以下の機能を具備させることで、なりすましクライアントのＩＰ通信を停止させる。

【００２４】ＡＲＰ応答にて許容外ＭＡＣアドレスが存在する場合に、ＤＨＣＰサーバ１０は、なりすましクライアント６０の通信拒否をスイッチングＨＵＢ３０に通知する。そして、スイッチングＨＵＢ３０は、内蔵する制御情報受信登録手段（図示せず）により、ＤＨＣＰ１０からの通知情報を抽出し内蔵するＭＡＣアドレス／ポート番号対応テーブル（図示せず）内にあるクライアント６０のＭＡＣアドレス通信可否状態（フラグ）をＮＧ（通信否）とする。これにより、スイッチングＨＵＢ３０は通信可否状態がＮＧのクライアント６０に対するスイッチング手段によるスイッチング動作を停止しその通

信を停止させる。

【００２５】次に、ＤＨＣＰサーバ１０の詳細構成を図２に示す。

【００２６】図２において本例のＤＨＣＰサーバ１０は、ＩＰアドレス割当てを許容するクライアントのＭＡＣアドレス（複数可）を記録しておく許容クライアントＭＡＣアドレスＤＢ（データベース）２０と、通常の動的ＩＰアドレス割り当てを行うＤＨＣＰサーバ処理部１６と、その割当て状況（ＩＰアドレスとＭＡＣアドレスとの組合せ）を記録しておく割当て済みアドレスＤＢ（データベース）１７と、現在、使用されているＩＰアドレス状況を確認する割当てアドレス確認部１２と、その使用状況を記録しておく使用アドレスＤＢ（データベース）１９と、状況確認後、許容外クライアントが検出された場合にそのクライアントに対してアドレスの解放を促すアドレス解放通知部１３と、許容外クライアントの通信を停止させる通信拒否通知部１４と、それぞれのデータの送受信する際の全般的な処理を行う通信処理部１５と、まだ割当てられていないアドレスを記録しているアドレスプールＤＢ（データベース）１８とから構成される。

【００２７】許容クライアントＭＡＣアドレスＤＢ２０には、予めＩＰアドレス割当てを許容するクライアントのＭＡＣアドレスが設定されている。これにより、クライアントからのサーバ検索要求受信時、そのＭＡＣアドレスとＤＢ内に設定されているＭＡＣアドレスを比較し、認証を行う。なお、許容クライアントＭＡＣアドレスＤＢ２０のＭＡＣアドレス登録内容（ＭＡＣアドレス）は、運用状態に応じて適宜書き換えられる（管理者等による）。すなわち、常に最新のＩＰアドレス割当てを許容するＭＡＣアドレス情報が得られる。

【００２８】ＤＨＣＰサーバ処理部１６により割当てられたＩＰアドレスは、対応するＭＡＣアドレスとともに割当て済みアドレスＤＢ１７に記録される。割当てアドレス確認部１２は、ＩＰアドレス割当て要求受付時に、アドレスプールＤＢ１８から選択した割当て予定ＩＰアドレスに対して、使用状況を確認するため、ＩＣＭＰ＿Ｅｃｈｏメッセージ（図３参照）を送付する。この使用状況は使用アドレスＤＢ１９に記録される。

【００２９】許容クライアントに割当てられたＩＰアドレスが許容外のクライアントに使用されるのを防止するために、ＩＰアドレス割当て後、定期的に、ＡＲＰパケット要求／応答メッセージ（図４参照）によって対応するＭＡＣアドレスによって検出する。それによって得られるデータ（ＩＰアドレスとＭＡＣアドレスとの組合せ）は、割当てアドレス確認部１２の一時的なメモリ内にＡＲＰテーブルとして登録される（図５参照）。このＡＲＰテーブルと、割当て済みアドレスＤＢ１７、許容クライアントＭＡＣアドレスＤＢ２０とが比較され判別される。許容クライアントＭＡＣアドレスＤＢ２０により、そのＭＡＣアドレスが現在、許容されているか判定され、割当て済みアドレスＤＢ１７により、ＭＡＣアドレスとＩＰアドレスとの組み合わせが正しいか判定される。

【００３０】実際に許容外のクライアントがＩＰアドレスを使用していた場合には、アドレス解放通知部１３及び通信処理部１５により強制ＩＰアドレス解放通知がそのクライアントに対して行われ、許容外クライアントの情報は使用アドレスＤＢ１９の許容外クライアント情報部分に記録され、その後、割当ては行わない。

【００３１】許容外クライアント検出時、通信拒否通知部１４は、ネットワーク内のスイッチングＨＵＢ３０に、通信拒否通知を送信する。通信拒否通知を受けたスイッチングＨＵＢ３０は、内蔵するＭＡＣアドレス／ポート番号対応テーブル内の通信可否状態（フラグ）にＮＧ（通信否）を設定する（図６参照）。

【００３２】次に、図１～図６とともに、動作シーケンスを示す図７を参照して本実施の形態の動作についてさらに詳細に説明する。

【００３３】前提条件として、サブネット内にＤＨＣＰサーバ１０が設置され、登録された許容クライアントＭＡＣアドレスは“ＡＡ　ＡＡ　ＡＡ　ＡＡ　ＡＡ　ＡＡ”とする。そして、許容クライアントをクライアント４０（ＭＡＣアドレス：ＡＡＡＡ　ＡＡ　ＡＡ　ＡＡ　ＡＡ）、許容外クライアントをクライアント６０（ＭＡＣアドレス：ＢＢ　ＢＢ　ＢＢ　ＢＢ　ＢＢ　ＢＢ）とし、共にＩＰアドレスが設定されていない状態（状態４０１、状態６０１）とする。なお、スイッチングＨＵＢ３０のポート１にＤＨＣＰサーバ１０、ポート２にクライアント６０、ポート３にクライアント４０が、それぞれ適切なネットワーク経路を介して接続されている。

【００３４】正当なクライアントであるクライアント４０は、ネットワークアドレスを構築するために、ＤＨＣＰサーバ１０に対してＤＨＣＰ＿ＤＩＳＣＯＶＥＲメッセージをブロードキャストする。

【００３５】ＤＨＣＰサーバ１０は、クライアント４０からのメッセージ中の送信元ＭＡＣアドレス（ＡＡ　ＡＡ　ＡＡ　ＡＡ　ＡＡ　ＡＡ）が、保持している許容クライアントＭＡＣアドレス（複数可。この場合、ＡＡ　ＡＡ　ＡＡ　ＡＡ　ＡＡ　ＡＡ）中にあるか照合する。照合の結果、許容クライアントであれば、ＤＨＣＰサーバ１０は割当て予定のＩＰアドレスに対して、ＩＣＭＰ＿Ｅｃｈｏメッセージにてアドレスの使用状況を確認し、未使用であればそのＩＰアドレスを設定した構成情報をＤＨＣＰ＿ＯＦＦＥＲメッセージにてクライアント４０に通知する。

【００３６】通知を受けたクライアント４０は、サーバＩＤなどを設定してＤＨＣＰ＿ＲＥＱＵＥＳＴメッセージをブロードキャストする。クライアント４０によって選択されたＤＨＣＰサーバ１０は、ＩＰアドレス（例え

ば、“１０．１．３２．１”）を指定してクライアント４０に対してＤＨＣＰ＿ＡＣＫ（ＯＫ）メッセージを送信する。

【００３７】ただし、割当てるＩＰアドレスがない等の要因で割当て不可能の場合は、ＤＨＣＰ＿ＮＡＫ（ＮＧ）メッセージが送信され、割当ては行われない。この時点でクライアント４０は、電源がまだＯＮ状態であり、ＤＨＣＰサーバ１０とのメッセージ送受信が可能である。これを状態４０２とする。

【００３８】一方、不正なクライアントであるクライアント６０（ＭＡＣアドレス：ＢＢＢＢ　ＢＢ　ＢＢ　ＢＢ　ＢＢ）が、ＤＨＣＰ＿ＤＩＳＣＯＶＥＲメッセージによりＩＰアドレス割当て要求を行うと、ＤＨＣＰサーバ１０は、クライアント４０に対して行ったと同様に、ＭＡＣアドレスによる許容クライアント判定を行う。しかし、クライアント６０は許容外のクライアントであるためＤＨＣＰサーバ１０は許容外クライアント通知を送信し、ＩＰアドレス割当ては行わない。これを状態６０２とする。

【００３９】ＩＰアドレス取得を失敗した許容外クライアント６０（そのユーザ）は、正当なＩＰアドレス割当てを受けているクライアント４０になりすますため、クライアント４０の電源をＯＦＦし動作不能状態（状態４０３）とし、自己のＩＰアドレスとしてクライアント４０のＩＰアドレス（“１０．１．３２．１”）を設定する。これを状態６０３とする。

【００４０】一定時間経過後、サーバ管理者によって設定された時間毎に、ＤＨＣＰサーバ１０は、ＡＲＰ要求メッセージをネットワーク上にブロードキャストする。

【００４１】クライアント４０は電源がＯＦＦされているため、ＡＲＰ応答メッセージはクライアント６０からのみ返却される。

【００４２】このＡＲＰ応答メッセージに含まれるＩＰアドレスとＭＡＣアドレスの組合せ（ＡＲＰテーブル）に対して、割当て済みアドレスＤＢ１７、許容クライアントＭＡＣアドレスＤＢ２０で保持しているデータとそれぞれ照合する。照合の結果、該当ＩＰアドレス（この場合、“１０．１．３２．１”）に対して違うＭＡＣアドレス（この場合、“ＢＢ　ＢＢ　ＢＢ　ＢＢ　ＢＢ　ＢＢ”）が存在した場合には、ＡＲＰ応答メッセージを返送したクライアント（クライアント６０）は許容外クライアントであるとして、そのＭＡＣアドレス（“ＢＢ　ＢＢ　ＢＢＢＢ　ＢＢ　ＢＢ”）に対して、アドレス解放通知部１３より強制ＩＰアドレス解放通知メッセージを送信する。

【００４３】解放通知メッセージ送信後、ＤＨＣＰサーバ１０は、通信拒否通知部１４よりスイッチングＨＵＢ３０に対して通信拒否通知メッセージを送信し、スイッチングＨＵＢ３０内のＭＡＣアドレス／ポート番号対応テーブル内の該当するＭＡＣアドレス（“ＢＢ　ＢＢ　ＢＢ　ＢＢ　ＢＢ　ＢＢ”）の通信可否状態をＮＧとして通信が行われないようにする（図６参照）。これにより、なりすましクライアント（正当なクライアント４０になりすましたクライアント６０）のＩＰ通信を停止させることができる。この状態を状態６０４とする。

【００４４】

【発明の効果】本発明によれば、ＤＨＣＰサーバによりＩＰアドレスの動的割当てを行っているネットワークにおいて、許容クライアント認証機能及び定期的なＡＲＰパケット送付により、クライアントに割当てたＩＰアドレスに対応するＭＡＣアドレス状況を確認し、許容外クライアントを発見した場合の対処機能としてＩＰアドレス解放通知機能、通信拒否通知機能及び通信拒否手段を具備することで、許容外クライアントのなりすましを防止することができる。

【図面の簡単な説明】

【図１】本発明の一実施の形態を示すネットワーク構成図である。

【図２】ＤＨＣＰサーバの詳細構成を示すブロック構成図である。

【図３】ＩＣＭＰ＿Ｅｃｈｏメッセージの構成例を示す図である。

【図４】ＡＲＰパケット要求／応答メッセージの構成例を示す図である。

【図５】ＡＲＰテーブルの構成例を示す図である。

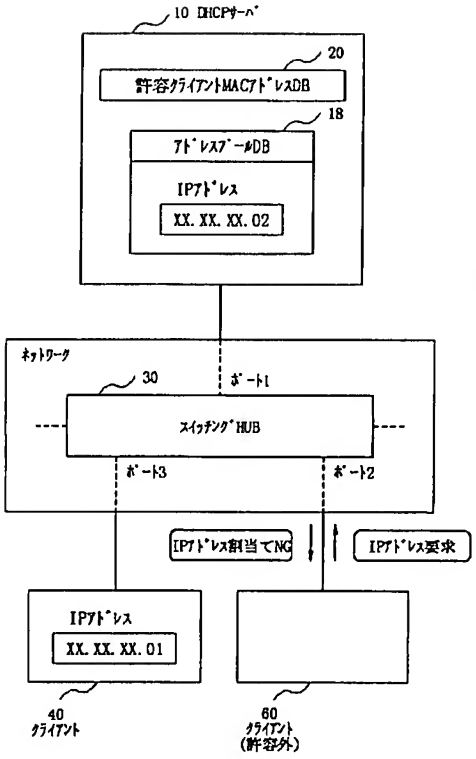
【図６】ＭＡＣアドレス／ポート番号対応テーブルの構成例を示す図である。

【図７】本発明の一実施の形態の動作シーケンスを示す図である。

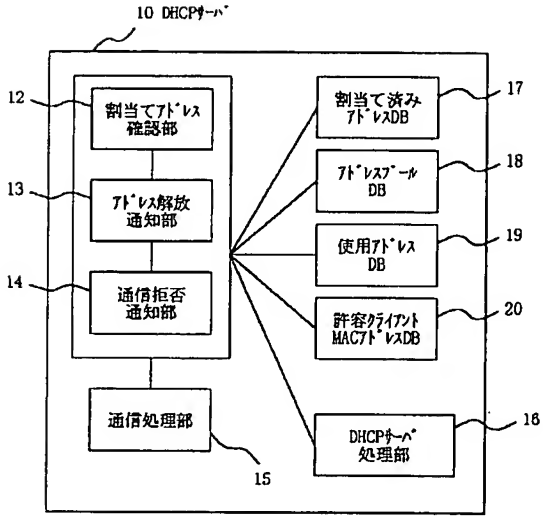
【符号の説明】

１０　ＤＨＣＰサーバ
１７　割当て済みアドレスＤＢ
１８　アドレスプールＤＢ
２０　許容クライアントＭＡＣアドレスＤＢ
３０　スイッチングＨＵＢ
４０，６０　クライアント

【図１】



【図２】



【図３】

ICMP (Echo) ﾒｯｾｰｼﾞﾌｫｰﾏｯﾄ

ﾀｲﾌﾟ	ｺｰﾄﾞ	ﾁｪｯｸｻﾑ
識別子		ｼｰｹﾝｽ番号
ﾃﾞｰﾀ		

【図４】

ARPﾊﾟｹｯﾄﾌｫｰﾏｯﾄ

ﾊｰﾄﾞｳｪｱﾀｲﾌﾟ		ﾌﾟﾛﾄｺﾙﾀｲﾌﾟ
ﾌﾟﾛﾄｺﾙｱﾄﾞﾚｽ長	ﾊｰﾄﾞｳｪｱｱﾄﾞﾚｽ長	要求or応答
送信元MACｱﾄﾞﾚｽ		
送信元IPｱﾄﾞﾚｽ		
ﾀｰｹﾞｯﾄMACｱﾄﾞﾚｽ		
ﾀｰｹﾞｯﾄIPｱﾄﾞﾚｽ		

【図５】

ARPﾃｰﾌﾞﾙ

IPｱﾄﾞﾚｽ	MACｱﾄﾞﾚｽ
AA. BB. CC. DD	EE FF GG HH II JJ
・	・
・	・
・	・

【図６】

MACアドレス／ポート番号対応テーブル

MACアドレス	ポート番号	通信可否状態
BB BB BB BB BB BB	02	NG
・	・	・
・	・	・
・	・	・

【図７】